投票所方式による電子投票システム

白石　旭　　田中　利清

ＮＴＴアドバンステクノロジ株式会社

１．はじめに

近年、社会の各分野において情報の電子化が進み、ネットワークが飛躍的に社会に浸透している。このような背景のもとで、選挙業務に対しても、それを電子化することで、開票の稼働を削減するとともに、開票時間を短縮することが期待されている。欧米を始め世界各国において電子投票システムの開発が進められ、一部の国においては既に実際の選挙に適用され始めている。我が国においても、模擬投票など実証実験を進めているシステムもあるが、各投票所と開票所がオンラインで結ばれていず、各所内業務の電子化に留まっている。

一方、インターネットの発展にともない、各家庭のパソコンから投票を行うことも可能な環境となりつつあり、学会レベルでの研究や議論が進められている。ただし、家庭と開票所をオンラインで結んだネットワーク方式の電子投票を実現するためには、本人認証の方式、本人認証のための情報を格納する IC カードなどの導入手段、脅迫や買収を防止する方式、通信履歴やアクセスポイントなどから投票者を特定することを防止する無記名性の確保方式など、解決すべき問題が散在し、国政選挙や地方自治体選挙に適用するには時期尚早と考える。

本研究開発においては、近い将来における、国政選挙や地方自治体選挙への適用を目標に、投票所に電子的な端末を設置し、投票所と開票所とをオンラインで結ぶ、「投票所方式による電子投票システム」を研究開発した。

本システムにおいては、現行選挙と同様の投票所に電子端末を設置し、投票者は投票所に出向いて投票を行う。本人認証は現行選挙の方式を踏襲することとし、例えば投票所の受け付けにて各投票者宛に郵送された投票整理券の提出を求め、それと有権者名簿とを突き合わせることにより本人認証を実施する。投票者は、本人認証終了後、現行選挙の投票用紙の代わりに IC カード（投票カード）を受け取り、投票カードを投票端末に挿入して投票を行う。投票カードに格納された投票情報は、投票所の出口端末からオンラインで集計サーバへ送信され、集計サーバのデータベースに格納される。投票締切後集計サーバにてデータベース内の投票情報が集計され、投票結果が出力される。

本研究開発により期待される効果としては、以下の３点が考えられる。

- 投票所における投票の運用および不正行為の監視等の投票管理者とその補助者や立会人の稼働は現行選挙とほぼ同じであるが、各投票所と開票所をオンラインで結ぶことおよび開票処理をコンピュータ上で実施することにより、投票所から開票所への投票箱の運搬および開票所における開票作業等の選挙運営に係わる稼働を大幅に削減することができる。
- また、各投票所と開票所をオンラインで結ぶことおよび開票処理をコンピュータ上で実施するこ

とにより、投票締切から投票結果判明までの時間を大幅に短縮することができる。

- 公職選挙法の改正を前提とするが、現行選挙における投票用紙への候補者名記入の代わりに、電子端末の画面上に表示した候補者の中から選択する方式を採用することにより、現行選挙で発生しやすい誤記や判読不能等による無効票が無くなる。

2．研究開発の目標と内容

本研究開発の目標は、国政選挙や地方自治体選挙に適用可能な電子投票システムを研究開発することである。選挙は国民が政治に参画する貴重な機会であることから、二重投票などの不正行為が防止でき、公平であり、プライバシーが保証されるなどの安全性の高いシステムが要求される。そのため、この要求条件を満たす電子投票プロトコルを研究開発し、その実現性を検証するとともに、電子投票システムの実装方法を確認するためにプロトタイプソフトウェアを開発する。なお、この電子投票プロトコルを研究開発する上で利用する主な既存技術は、暗号・認証技術である。

電子投票プロトコルの研究開発における主要な研究開発項目を以下に示す。

① 無記名性の実現

異議申し立てや二重投票の防止を実現する上で、無記名性を損なわない方式を検討する。即ち、異議申し立てや二重投票の防止を実現するためには、投票情報を識別する手段が必要であるが、この投票情報識別手段から投票者が特定され、無記名性が損なわれる危険性がある。そのため、無記名性を損なうことなく、投票情報を識別する手段を実現する方式を検討する。

② 異議申し立ての実現

集計に対する投票所内に設置する受付端末、投票端末、出口端末は、投票者の目の届く範囲にあるため、不正行為が行われないように投票者本人が監視できる。これに対して、集計サーバは、投票者の目の届かない場所に設置して運用されるため、投票者の不信を招きやすい。このため、立会人や投票者が関与できる出口端末にて、集計サーバで投票情報の削除や改ざんや水増しが行われていないかを監視し、不正を検出した場合には集計サーバに対して異議申し立てを行う方式を検討する。なお、異議申し立て時のプライバシ保護（無記名性保証）の観点から、当該投票所に関与した全投票者の代わりに出口端末が異議申し立てを実行することとする。

③ 二重投票の防止

一人の投票者が二票以上の投票を行う二重投票を防止する方式を検討する。主な二重投票の手段としては、一枚の投票カードを用いて二回投票する、複写などにより偽造投票カードを作成して密かに投票所に持ち込む、などが考えられる。

④ 安全性の実現

上記の無記名性や異議申し立ての実現および二重投票の防止のために、暗号・認証技術を使用する。この暗号・認証で使用する各種の鍵情報を安全に保管および配布する方式を検討する。

3．本年度の活動状況

３．１　電子投票プロトコルの研究開発

上記研究開発項目について検討を行い、その結果を電子投票プロトコル仕様書としてまとめた。主要な検討結果を以下に示す。

３．１．１　無記名性の実現

無記名性を保証するために、投票カードには投票者を特定できる情報を一切格納しない。

ただし、異議申し立ておよび二重投票の防止を実現するためには、個々の投票情報を識別するための手段が必要である。これを無記名性を損なうことなく実現するために、投票端末で乱数を生成し、この乱数を投票情報を識別するための手段として使用する。

なお、投票チケットサーバで乱数を生成し、これを投票チケットに包含する方式も考えられるが、この投票チケットが格納された投票カードが複製されて、正規の投票カードに混入された場合、正規に投票した投票情報が多数無効化されることになるため、本システムでは、投票者が投票端末で投票を行い、投票情報が生成される段階で乱数を生成して付加する方式を採用した。

選挙区の有権者数に対して、乱数の桁数を十分大きく取ることにより、同一選挙区内の複数の投票端末で、個別の乱数の種のもとで同一の乱数が生成される確率は極めて小さくなる。しかし、一票の票の重みを考慮した場合、いかに確率が小さくても同一の乱数が生成されたことにより、ある投票情報が無効化されることは許されない。このため、投票チケットサーバにて投票チケットを生成する時に、投票チケットにシーケンス番号を包含し、このシーケンス番号を、万一乱数が一致した場合に、投票情報をさらに識別するための手段として使用する。

ただし、受付端末の操作者が投票チケット内のシーケンス番号を見ることができると、投票者とシーケンス番号、シーケンス番号と投票情報とのマッピングが可能となり、無記名性を損なう恐れがある。このため、投票チケット内のシーケンス番号は暗号化して、投票所受付の投票管理者に見えないようにし、投票端末のみで復号する。

なお、このシーケンス番号だけで投票情報を識別する方法も考えられるが、上記の乱数の場合で議論したのと同様、この投票チケットが格納された投票カードが複製されて、正規の投票カードに混入された場合、正規に投票した投票情報が多数無効化されることになるため、本システムでは、乱数とシーケンス番号の二つで投票情報を識別する方式を採用した。

３．１．２　異議申し立ての実現

投票所内の受付端末、投票端末、出口端末は、投票者の目に届く範囲にある。しかし、集計サーバは投票者の目の届かない場所に設置されるため、投票者は集計サーバでの不正処理が心配となる。現行選挙では、開票時の不正を監視するために立会人を置くとともに、それ以外の投票人の傍聴も可能である。本システムにおいても、立会人の監視の下で開票が行われることを前提としているが、集計サーバの処理内容に不正がないかを投票者自身から納得できない。このため、投票者も監視できる出口端末で、集計サーバによる投票情報の削減、改ざん、水増しを監視する異議申し立ての方式を実現する。

異議申し立ての実現方式として以下の２つの方式が考えられる。ただし、以下の議論における投票情報は、投票した候補者名とともに、上記の乱数およびシーケンス番号を含むものとする。また、集計サーバ署名は、集計サーバが出口端末から受信した投票情報に対し、集計サーバ署名秘密鍵を用いて生成した署名である。

- 直接方式・・・投票者は、投票情報および集計サーバ署名を格納した投票カードを持ち帰る。集計サーバは、集票してデータベース上に保持している全ての投票情報の一覧を、FTP 等により一般投票者に公開する。投票者は、公開された投票情報の一覧の中に自分の投票情報があることを確認する。自分の投票情報が公開された投票情報の一覧に存在しない場合、集計サーバに異議申し立てを行う。集計サーバは、異議申し立てに添付された集計サーバ署名を検証し、集計サーバ署名が正しければ、異議申し立てを認めて、異議申し立ての投票情報をデータベースに追加する。
- 代理人方式・・・投票者は、投票情報および集計サーバ署名を格納した投票カードを投票箱に投函する。集計サーバは、集票してデータベース上に保持している全ての投票情報の一覧を、FTP 等により代理人に公開する。代理人は、投票箱に投函された全ての投票情報が、公開された投票情報の一覧の中にあることを確認する。投票情報が公開された投票情報の一覧に存在しない場合、集計サーバに異議申し立てを行う。集計サーバは、異議申し立てに添付された集計サーバ署名を検証し、集計サーバ署名が正しければ、異議申し立てを認めて、異議申し立ての投票情報をデータベースに追加する。

上記２方式のうち、直接方式にて異議申し立てを行った場合、異議申し立てをした人が誰に投票したかが分かってしまうため、無記名性を損なう。また、投票者が持ち帰った投票カードを証拠として、票の買収あるいは脅迫の行われる危険がある。従って、本システムにおいては、代理人方式を採用した。ただし、代理人が人手で上記投票情報一覧のチェックを行うことは、現行投票における開票と同等の稼働および時間を費やすこととなり、電子投票を導入する意味がなくなる。このため、本システムでは、出口端末が代理人の処理を実行する方式とした。

異議申し立ての具体的実現方式を以下に示す。

① 投票時

- 出口端末は、投票カードから投票情報を読み出し、投票情報を集計サーバへ送信する。
- 集計サーバは、出口端末から受信した投票情報に対する集計サーバ署名を生成し、集計サーバ署名を出口端末へ送信する。また、投票情報をデータベースに格納する。
- 出口端末は、上記投票カードから読み出した投票情報と、集計サーバから受信した集計サーバ署名を、データベースに格納する。

② 開票時

- 集計サーバは、データベース内の投票情報の一覧を FTP で公開する。
- 出口端末は、自データベース内の投票情報の全てが、集計サーバから公開された投票情報一覧の中に存在していることを確認する。全て存在している場合は、承認情報を集計サーバへ送信する。存在しない投票情報を検出した場合、該当の投票情報と集計サーバ署名を含む異議申し立て情報を集計サーバへ送信する。
- 集計サーバは、出口端末から異議申し立て情報を受信した場合、異議申し立て内の集計サーバ

署名を検証し、署名検証に成功した場合は、異議申し立てされた投票情報をデータベースに格納し、署名検証に失敗した場合は、対応する投票情報を破棄する。

- 集計サーバは、再度、データベース内の投票情報の一覧を FTP で公開する。
- 出口端末は、自データベース内の投票情報の全てが、集計サーバから公開された投票情報一覧の中に存在していることを確認する。全て存在している場合は、承認情報を集計サーバへ送信する。存在しない投票情報を検出した場合、凍結情報を集計サーバへ送信する。
- 集計サーバは、出口端末から凍結情報を受信した場合、開票処理を凍結する。（この後、開票管理者による調査が行われる。）

上記異議申し立て方式では、集計サーバによる投票情報の水増しを検出することができないため、以下の手順を追加する。

- 出口端末による、１回目の投票情報チェックの結果に基づく集計サーバへの送信情報（承認情報または異議申し立て情報）に、自出口端末の投票情報数を包含する。
- 集計サーバによる、２回目の投票情報一覧の公開時に、全ての出口端末から受信した各出口端末の投票情報数を包含する。
- 出口端末は、２回目の投票情報チェック時に、集計サーバから公開された自出口端末の投票情報数が正しいこと、および集計サーバから公開された投票情報の総数が公開された各出口端末の投票情報数の合計に等しいことを各々が検査し、不一致を検出した場合には、凍結情報を集計サーバへ送信する。（この後、開票管理者による調査が行われる。）

３．１．３　二重投票の防止

投票者が当該投票所で投票をする資格があり、かつ１回目の投票であることの確認は、現行選挙の方式を踏襲することとし、例えば投票所受付にて各投票者宛に郵送された投票整理券の提示を求め、投票管理者がその投票所に割り当てられた選挙人名簿に投票済みの印を記入することにより行う。

その後、本システムでは、上記確認の終了した投票者に対して、投票者が受付端末で受付端末署名を書き込んだ投票カードを交付する。この受付端末署名は、投票端末において検証されるため、事前に投票チケットを複写するなどして偽造した投票カードを投票所に持ち込んでも、受付端末署名が書き込まれていないために投票端末で偽造が検出されるので、投票することはできない。なお、受付端末署名は、受付端末が、投票カードから投票チケットを読み出し、この投票チケットに対して、受付端末署名秘密鍵を用いて生成した署名である。

ただし、投票端末で受付端末署名がないことを検出した場合、あるいは受付端末署名の検証に失敗した場合、投票カードの不良やシステムの動作不良と偽造カードとの切り分けを、投票所で即座に実施することは運用的に困難であることから、投票を行う権利を尊重して、投票カードを再交付せざるを得ない。このように、受付端末で最初に正規の交付された投票カードと、偽造カードの代わりに再交付された２枚目の正規の投票カードを使用して、二重投票が行われる危険性がある。本システムでは、投票所の出口で投票管理者が投票者から投票カードを１枚のみ受け取り、その投票カードを出口端末に挿入して、投票情報を集計サーバへ送信するので、２枚の投票カードの使用に

よる二重投票を防止することができる。

また、１枚の投票カードを用いて２回投票しようとしても、１回目の投票時に、投票端末にて投票カード内の投票チケットと受付端末署名を消去するため、２回目の投票の開始において、投票端末に投票を拒否される。

更に、投票チケットに、選挙毎に決定する選挙識別子に対して投票チケットサーバ署名秘密鍵を用いて生成した投票チケットサーバ署名を包含することにより、投票チケットの偽造を困難にしている。

また、回線上の投票情報のパケットをコピーし、通信処理上のセキュリティホールを見つけて、同一の投票情報を送信することにより、集計サーバのデータベースに複数格納することが考えられる。このため、集計サーバは開票の始めに、データベース上の投票情報の重複を、乱数およびシーケンス番号の照合によって排除する。

３．１．４　安全性の実現

暗号・認証に使用する鍵を安全に保管し、配布するために、これらを IC カード（セキュリティカード）に格納する。さらに、IC カードには、IC カードの所有者を認証するための情報として、所有者の識別子とパスワードを格納する。

IC カードの種類は、投票管理者や開票管理者のための管理者用 IC カードと、投票立会人や開票立会人のための立会人用 IC カードの２種類を設ける。管理者用 IC カードには、管理者の識別子とパスワード、立会人（複数）の識別子、鍵情報を格納する。立会人用 IC カードには、立会人の識別子とパスワードを格納する。

また、現状の公職選挙法との整合性を考え、例えば投票端末に対しては、１枚の管理者用 IC カードと５枚の立会人用 IC カードとを発行し、投票端末の運用開始には、管理者用 IC カードの認証と、２枚以上の立会人用 IC カードの認証を必要とする。

３．２　プロトタイプソフトウェアの開発

上記電子投票プロトコルの実現性を検証するとともに、電子投票システムの実装方法を確認するためにプロトタイプソフトウェアを開発した。

ただし、開発期間および開発稼働の制約から、下記の条件を設定した。

- IC カードは使用せず、投票カードおよびセキュリティカードの機能を FD で代替する。また、セキュリティカードを用いた管理者や立会人の認証は行わない。
- 操作者とのインタフェースは GUI を使用せず、コマンドライン入出力で代替する。また、タッチパネルを使用せず、キーボード入力で代替する。

プロトタイプソフトウェアの構成は以下の通りである。

①　投票チケットサーバ

［機能］

- 投票チケットを生成し、投票カードに格納する。投票チケットは、選挙識別子に対する投

票チケットサーバ署名と暗号化されたシーケンス番号から構成する。

［運用］投票に先立ち、投票チケットサーバを用いて、有権者数分の投票カードを作成する。

② 受付端末

［機能］

- 投票カードから投票チケットを読出し、投票チケットに対する受付端末署名を生成して、投票カードに格納する。

［運用］投票所受付では、各投票者宛に郵送された投票整理券などにより本人認証を行った後、受付端末を用いて、投票カードに受付端末署名を格納して、投票カードを投票者に手渡す。

③ 投票端末

［機能］

- 投票カードから受付端末署名と投票チケットを読出し、受付端末署名の検証および投票チケットサーバ署名の検証を行う。
- 候補者情報を表示し、投票者が選択した投票内容に基づいて投票情報を生成する。投票情報は、投票内容と、投票チケットサーバが発行したシーケンス番号と、投票端末が生成した乱数から構成する。
- 投票情報に対する投票端末署名を生成し、投票情報と投票端末署名を投票カードに格納する。

［運用］投票者は、投票所受付で受け取った投票カードを投票端末に挿入し、画面に表示された候補者から選択して投票する。

④ 出口端末

［機能］

- 投票カードから投票情報と投票端末署名を読出し、投票端末署名の検証を行う。
- 投票情報を暗号化し署名を添付して、集計サーバへ送信する。
- 集計サーバから集計サーバ署名を受信し、集計サーバ署名の検証を行う。
- 投票情報と集計サーバ署名を出口端末データベースに格納する。
- 集計サーバが公開した投票一覧情報と出口端末データベースの内容との照合を行い、その結果に基づいて承認情報または異議申し立て情報を集計サーバへ送信する。

［運用］投票所出口にて、投票者から投票カードを１枚のみ受け取り、出口端末を用いて、投票情報を集計サーバへ送信する。また、集計サーバによる集計結果のチェックを行い、不正を検出した場合に、異議申し立て情報を集計サーバへ送信する。

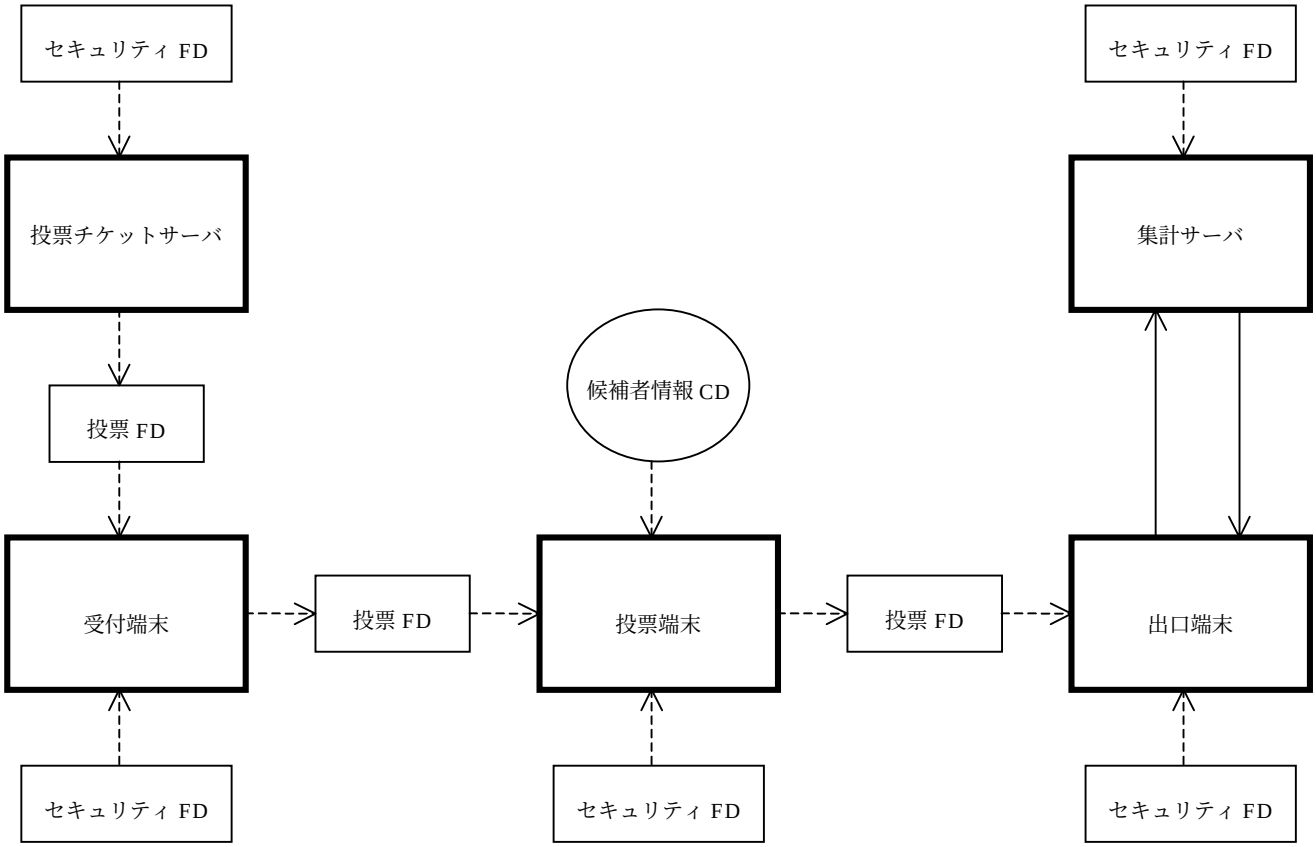
⑤ 集計サーバ

［機能］

- 投票情報を出口端末から受信し、署名の検証および復号化を行う。
- 投票情報に対する集計サーバ署名を生成し、集計サーバ署名を出口端末へ送信する。
- 投票情報を集計サーバデータベースに格納する。
- 集計サーバデータベース上の投票情報から有効投票情報を抽出する。
- 有効投票の一覧情報を公開する。
- 出口端末から承認情報または異議申し立て情報を受信し、異議申し立ての場合は集計サーバ署名を検証して、集計サーバデータベースへ反映する。
- 候補者毎の得票数を集計する。

［運用］集票処理の開始および終了を行う。集計結果を公開し、出口端末の承認を得た後、候補者毎の得票数を集計する。

電子投票システムのプロトタイプソフトウェア構成図を以下に示す。



（注：　読出し／書込み　------≫　　通信　⟶　　）

図　　プロトタイプシステム構成図

３．３　電子投票システムの評価

上記プロトタイプシステムを用いて、電子投票プロトコルおよびシステムの評価を行った。評価結果は以下の通りである。

①　安全性の評価

- 下記の観点から二重投票の防止ができることを確認した。
  - １枚の投票 FD で２回投票することの防止
  - 受付端末署名が格納されていない偽造投票 FD で投票することの防止
  - 投票チケットが格納されていない偽造投票 FD で投票することの防止
  - データベースに重複して格納された投票情報の削除
- ３０００件の疑似乱数を生成して値の重複、規則性が無いことを確認し、無記名性を損なうことなく投票情報を識別するための手段として乱数を使用することの妥当性を検証した。

- 下記の観点から異議申し立てが実現されていることを確認した。
  - 正当な異議申し立て情報を集計サーバデータベースに反映できること
  - 不当な異議申し立て情報を集計サーバが棄却できること

② 性能評価

- 集票（出口端末→集計サーバ）のターンアラウンド時間は、平均２．８秒であり、その内訳は出口端末処理時間が２．７秒、残りが通信時間と集計サーバ処理時間であった。ただし、出口端末処理時間の大部分は FD からの読出し時間であった。
- 集計サーバデータベース上での有効投票情報抽出時間は、投票情報１０００件～３０００件で２分～５分であり、ほぼ情報件数に比例して増加することが分かった。また、出口端末データベース上での公開された投票一覧情報照合時間は、同じく投票情報１０００件～３０００件で３分～９分であり、これもほぼ情報件数に比例することが分かった。
- 照合結果に基づく承認処理のターンアラウンド時間は、平均３．８秒であり、その内訳は出口端末処理時間が１．０秒、集計サーバ処理時間が２．８秒であった。
- 照合結果に基づく異議申し立て処理のターンアラウンド時間は、平均５．８秒であり、その内訳は出口端末処理時間が２．８秒、集計サーバ処理時間が３．０秒であった。

４．外部発表及び成果物

４．１　外部発表

[1] 白石旭，田中利清，“投票所方式による電子投票システム”，Cyber Security Magazine，Vol.2，pp28-31，1999.

４．２　成果物

[1] 研究開発報告書（研究開発編、ソフトウェア開発編、取扱説明書編）

[2] 電子投票プロトタイプシステム

- 投票チケットサーバソフトウェア
- 受付端末ソフトウェア
- 投票端末ソフトウェア
- 集計サーバソフトウェア
- 出口端末ソフトウェア

５．今後の課題

今後の課題としては以下の項目が上げられる。

- 今期は、IC カードの代替として FD を用いて、鍵情報の保管・配布および投票チケット・投票情報の持ち運びを行った。特に鍵情報の安全な保管・配布のためには、IC カードの導入が必須

である。また、IC カードの導入と同期して、IC カードを用いた管理者および立会人の認証の実装も必要である。

- 今期は、操作者とのインタフェースとして、テキストメッセージの出力およびキーボード入力を使用している。今日 GUI インタフェースは当然であり、電子投票システムとして投票者に受け入れられるためには、インタフェースの簡易な GUI 化が必要である。また、老人や主婦が違和感なく操作できることも必要であり、諸外国の実用化・実証実験の例からもタッチパネルの実装が必要と考える。
- 今期のプロトタイプソフトウェア開発においては、仮投票のサポートなど現行公職選挙法で規定されている各種バリエーションを可能な限り取り入れたが、点字投票と郵便投票に対しては対応できていない。今後電子投票専用端末を試作する場合には、目の不自由な方への対応を検討する必要がある。また、郵便投票に関してはその代替としての在宅投票の方式を検討したい。
- 今期のプロトタイプソフトウェア開発においては､町村レベルの地方選挙を適用対象としている。これを県や国政レベルの全国規模に適用するためには、集計サーバでの集計結果をさらに集約する階層化したシステム構成の方式検討が必要である。

６．まとめ

本研究開発においては、平成１１年度は２年計画の初年度であり、電子投票プロトコルの確立と、電子投票プロトコルを検証するためのプロトタイプソフトウェアの開発および評価を実施した。電子投票プロトコルの開発においては、①二重投票の防止と無記名性の実現を両立させること、②トラブル発生時の投票カード再発行を利用した二重投票を防止すること、③投票者の目の届かない場所で処理が行われる集計サーバの不正をチェックすること、に多大な検討を要した。①に対しては、投票端末で生成した乱数と投票チケットに包含されたシーケンス番号を併用することにより、無記名性を損なうことなく、投票情報を識別する方式を確立した。②に対しては、投票情報を出口端末から集計サーバへ送信することにより、投票カード再発行を利用した二重投票を防止する方式を確立した。③に対しては、集計サーバの集計結果を出口端末が検証し、不正検出時には異議申し立てを行う方式を確立した。

７．参考文献

[1] 藤崎英一郎, 太田和夫, 岡本龍明, ：投票所を仮定した実用的な電子投票方式, 信学技報, ISEC93-24, 1993

[2] 藤岡淳，藤崎英一郎，岡本龍明, ：電子投票方式，NTT R&D，44，No.10，pp939-946，1995.